PCSRF Meeting Notes

Wednesday August 21, 2002 8:00 AM – 5:00 PM ET
Hosted by AGA
American Gas Association Headquarters
Hall of States Building, Washington, D.C.

Participants

Fred Proctor and Keith Stouffer (NIST MEL)
Jerry Stenbakken and Art Griesser (NIST EEEL)
Michael McEvilley (DAC)
Dave Teumim (ISA)
Joe Weiss (KEMA Consulting)
Bill Miller (MaCT)
Dan Carnahan (Rockwell Automation)
Paul Blomgren (Mykotronx)
David Saunders (Westin)
Bill Rush, John Kinast, and Joe McCarty (GTI)
Ali Quraishi (AGA)
Peter Sargent (PreVal)
Bryan Singer (EnteGreat)
Dennis Holstein (Opus Publishing)

Purpose

To review the progress and direction of the group; review the Security Profile Specification (SPS) document; review the AGA SCADA cryptography report; share status and plans among participants; and plan the timing and agenda for next face-to-face meeting.

Web Site Updates

All the information on the PCSRF site is now password protected. Most of the information on the site is not sensitive and can be found elsewhere on the web, but there is a lot of information gathered in one place. If you don't have a username and password yet, please follow the directions located at http://www.isd.mel.nist.gov/projects/processcontrol/members.html to request one.

The minutes from the past meeting were added to the web site.
The minutes from the Vulnerability Assessment Methodology meeting were added to the web site.
The presentations from the August 21 meeting were added to the web site.
The Security Profile Specification (SPS) document was added to the web site.

Opening Remarks

Fred Proctor (NIST) started the meeting restating that the PCSRF has to focus more on its outputs. The outputs of the PCSRF will be Protection Profiles (PPs) for the process control industry.

Security Profile Specification (SPS) Review Presentation- Michael McEvilley, Decisive Analytics

The material from this presentation is on the PCSRF web site at
http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/21-Aug-2002/SPS.pdf

Michael McEvilley (DAC) reported on the status of the SPS document. The SPS was updated based on the information gathered at the National Center for Manufacturing Sciences (NCMS) sector workshop that was held in Dearborn, Michigan on June 27, 2002. The current SPS document is on the PCSRF web site at http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/SPS-29-Aug.doc

During his presentation Michael pointed out the following:

- A study by the Naval Research Lab (NRL) reported that of the 50 security flaws that were found, 22 of them were specified into the design of the system.

- Security is a process and must be engineered into the system. How do you know that there is security in the system. with assurance. How do you get assurance? It has to be engineered into the system.

- A validated SPS can be translated to a Common Criteria Protection Profile. When the SPS is complete, it will be translated into the more formal language of a Protection Profile. Ideally this is a "desk exercise".

Experiences Translating Security Requirements into Protection Profiles Presentation- Peter Sargent, PreVal Specialist

The material from this presentation is on the PCSRF web site at
http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/21-Aug-2002/Sargent.pdf

Peter Sargent (PreVal) reported on his experience of translating security requirements, such as those being assembled in the SPS document, into Protection Profiles. This is a 4-step process: write requirements, vet these with domain experts, (iterate previous two steps), convert to a PP, vet this with experts (iterate previous two steps).

There is a large push from the federal government (especially Homeland Security) for protection profiles.

Peter reported that there is a lot of good information located at the Committee on National Security Systems (formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC)) site located at www.nstissc.gov

Peter also mentioned FIPS 140-2 validation for cryptography. Additional information can be found at http://csrc.nist.gov/cryptval/140-2.htm

Multi-hop Peer-to-Peer WLAN Pilot Test and discussion on Multi-hop Peer-to-Peer WLAN SBUE Protection Profile Presentation- Bill Miller, MaCT

The material from this presentation is on the PCSRF web site at at
http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/21-Aug-2002/Miller.pdf

Bill Miller reported on his experiences on a secure multi-hop wireless pilot test, which he likened to a "wireless VPN" (virtual private network). The pilot test was performed on an ABB DCS system. They performed Wave Relay feasibility testing on 802.11a (900 MHz) and 802.11b (2.4 GHz) wireless

standards. They also performed some testing on PC Anywhere for remote monitoring and control testing. Upon testing it was determined that 802.11a did not work as well as 802.11b in an environment with obstructing walls, and they decided on 802.11b as a result.

Bill reported that there was no measurable latency in the system when using the Blowfish block cipher with 128-bit blocks, both qualitatively and using network analysis tools. In Bill's system there were 5 nodes, and a maximum of three hops. Michael McEvilley asked about the scalability of the approach. Bandwidth decreases as the number of hops increases. This question will undoubtedly be answered in field tests.

AGA SCADA Cryptography Report - Bill Rush, Gas Technology Institute

Bill Rush (GTI) gave a quick report on the status of the AGA SCADA Cryptography effort, which will be published as AGA Report No. 12. Additional information can be found at http://www.gtiservices.org/security/report/index.shtml

SPS Document Review

The group provided comments on the current SPS document. Credit goes to Bill Miller for being the only one to forward comments to Michael. The group made general comments on the document, which Fred Proctor asked be submitted as specific requests for changes to the document. Only when comments are made this specifically can the document be propelled forward.

The group noted that a set of definitions (a glossary) would be helpful. We can use the NIST FIPS-140 and AGA additions, and may not need to extend these. Dan Carnahan noted that IEC 61069 would be another reference, and he will forward this to Fred.

The group spent considerable time on the "Operational Security Environment" section, for which domain experts will have the most to offer. Much of the entries currently in this section are instructional placeholders that need to be fleshed out by this group. Michael will mark these with "Application Note:" flags to make it more obvious to reviewers where work needs to be done. Michael will also make changes to the formatting and organization.

Dave Teumim initiated discussion on the limited audience that could understand the language of the SPS document. Joe Weiss agreed and suggested that we include a concrete example. Michael McEvilley stated again that the purpose of the SPS is to drive the writing of a protection profile, and is not intended as a standalone document. However, the group agreed that the more accessible the SPS document, the easier it will be for us to get comments and review from desk experts. Bill Rush volunteered John Kinast and Joe McCarty to work on definitions and examples.

Participant Status Updates

Michael McEvilley (DAC) reported that at the Boston Open Group meeting, it was stated that encryption can be implemented now without glitches because of the fast processor speeds of currently available processors.

Bill Rush (GTI) volunteered that he, John Kinast Joe McMarty will put together a definition of terms list.

Art Griesser (NIST) suggested that the PCSRF should pick a specific Vulnerability Assessment Methodology (VAM) for our Protection Profile development. It was noted that a VAM serves two purposes. For us, it is the basis for the development of our security requirements and protection profiles.

For companies, a VAM would initiate a review that would culminate in the purchase of products to which protection profiles apply. So, it is important that we be aware of what recommendations are likely to result from a VAM, so that our PPs will apply.

Keith Stouffer (NIST) reported on the updates to the PCSRF web site and the status of the NIST process control testbeds. NIST has several testbeds, one in the Manufacturing Engineering Laboratory for which SCADA equipment is currently being purchased, and one in the Electronics and Electrical Engineering Laboratory that Jerry Stenbakken described. Jerry noted that he expects by November to have prototype "bumps in the cord" from Paul Blomgren and Dennis Holstein, that can be tried out in the testbeds.

Dan Carnahan (Rockwell) noted that the maintenance part of the product life cycle came up during the NCMS workshop. Remote diagnostics are expected to play an important part in reducing maintenance costs, but they introduce security holes. How can procurement be made aware of security requirements for remote diagnostics? The group noted that these cross-cutting issues need to come to the attention of top management, and perhaps this would result from a company's VAM exercises.

Interoperability was brought up, and participants in yesterday's AGA SCADA Encryption working group meeting noted that this is a difficult problem that will not be addressed in the early releases of AGA Report No. 12. The PCSRF needs to be aware that security requirements and policies are understood throughout a system of heterogeneous products. Codifying these requirements and policies is one job of a protection profile.

Bryan Singer (EnteGreat) reported that he is working on establishing an ISA subcommittee. Currently a ballot for the establishment of a security committee is out for vote, and he expects that it will pass.

Dave Teumim (ISA) reported that the ISA security course went very well.

Michael McEvilley (DAC) added that we should look at getting Microsoft (a .NET person) to come to the next PCSRF face-to-face meeting. Joe Weiss (KEMA) thought that he could track down a Microsoft person to come talk at our next meeting. Michael McEvilley and Bill Miller thought that they could do the same.

Joe Weiss reported that Rolf Carlson of Sandia is working on protection profiles with IEC TC57 WG15. Jerry Stenbakken responded that he will look into this, find out the status, and recommend any liaison activity.

Sector Workshops

The National Center for Manufacturing Sciences (NCMS) sector workshop was held at the Dearborn Inn on June 27, 2002 in Dearborn, Michigan. Approximately 30 attendees registered with representation from Caterpillar, Delphi, Wells Spring Solutions, Rockwell, Square D, GM, Daimler Chrysler, and others.

Next Meeting

The next PCSRF meeting will be a conference call on September 23 at 10:30 am EST. Additional information on the next meeting will also be posted in the Upcoming Meetings section of the PCSRF web site.

The next face-to-face meeting is proposed to be at the Chicago ISA meeting between October 21 – 23, 2002. Additional information on the next face-to-face meeting will also be posted in the Upcoming Meetings section of the PCSRF web site.

Action Items

1. Keith Stouffer and Fred Proctor will post the following on the PCSRF web site: 3 presentations; Joe Weiss' Congressional testimony; NRC "Branscomb Report" on CIP; Sandia SCADA key management report

2. Jerry Stenbakken will follow up with Rolf Carlson on the Protection Profiles

3. Bill Rush will send Fred Proctor the AGA glossary

4. Fred Proctor will extract the glossary from FIPS-140, if possible

5. Dan Carnahan will send IEC 61069 to Fred Proctor

6. Michael McEvilley will go over the SPS document and make editorial changes discussed during the meeting

7. John Kinast and Joe McCarty will come up with examples to clarify the SPS, per Bill Rush's kind volunteering

8. Fred Proctor will arrange the next PCSRF meeting, a conference call for September 23 at 10:30 am EST

9. Fred Proctor will call Lois Ferson at ISA to see about scheduling the next face-to-face meeting at the Chicago ISA meeting between October 21 – 23, 2002